Sicherheit für mobile Computer

Winfried Naumann | Computer- und Medienservice, Systemsoftware und Kommunikation | w.naumann@cms.hu-berlin.de

Mobile Rechner sind beim Transport und bei der Nutzung in verschiedenen Netzen größeren Gefahren ausgesetzt als stationäre Arbeitsplatzrechner. Wie müssen die Benutzer und die Administratoren sich darauf einstellen?

Dieser Beitrag konzentriert sich auf die Sicherheit von Notebooks, weniger auf die kleineren mobilen Geräte (PDAs, Smartphones, Mobiltelefone), obwohl diese Geräte wegen ihrer zunehmenden Fähigkeiten immer mehr in Sicherheitsüberlegungen einbezogen werden müssen. Noch ist es aber so, dass der Benutzer auf der Betriebssystem- und Software-Seite kaum eingreifen kann, um diese Geräte sicher zu betreiben. Mögliche Risiken kann er aber durch verantwortungsbewussten Einsatz verringern.

Für die Absicherung mobiler Computer gilt erst einmal uneingeschränkt alles, was in den anderen Artikeln dieses Heftes zum Thema geschrieben steht. Dennoch gibt es einige Besonderheiten für mobile Rechner:

- Dienstliche und private Nutzung vermischen sich hier häufig.
- Der Einsatz erfolgt an verschieden Orten und in wechselnden Netzen.
- Es werden drahtlose (oft sehr leicht abhörbare) Netzverbindungen genutzt.
- Die Gefahr von Verlust, Diebstahl oder Beschädigung ist größer.
- Die Anforderungen an die Verfügbarkeit der Rechner sind höher.

Welche Auswirkungen hat das auf die Sicherheitsanforderungen?

Vermischung von dienstlicher und privater Nutzung

Während private Dinge vom stationären Arbeitsplatzrechner noch recht einfach fernzuhalten sind, ist das auf einer längeren Dienstreise mit einem Notebook kaum machbar. Auch bei der privaten Nutzung von Computern sollte man sich mit gut abgesichertem Rechner und Verantwortungsbewusstsein durch das Netz bewegen. Dabei werden andere Web-Seiten besucht und teilweise andere Programme benutzt, die in der Nachbarschaft von vertraulichen dienstlichen Daten durchaus ein Sicherheitsrisiko darstellen können. Was folgt daraus?

- Wenn es möglich ist, vermeiden Sie die private Nutzung von dienstlichen Computern trotzdem oder beschränken Sie sie verantwortungsbewusst auf das Minimum. Dieser Rechner sollte nur vom Besitzer selbst, nicht auch noch von Familienmitgliedern und Freunden genutzt werden. Private und dienstliche Nutzung dürfen nicht parallel erfolgen, sondern nur zeitlich nacheinander. Es versteht sich von selbst, dass man nur mit einem normalen Benutzer-Account (ohne administrative Rechte) arbeiten sollte, um weitere Risiken minimal zu halten.
- Vertrauliche dienstliche Daten auf den angeschlossenen Speichermedien (Festplatten, USB-Sticks) müssen unzugänglich sein. Das ist sehr einfach zu gewährleisten, wenn diese Daten in verschlüsselten Containern oder auf verschlüsselten Laufwerken liegen, die nur dann geöffnet werden, wenn Sie mit diesen Dateien arbeiten (siehe z. B. den Artikel zu TrueCrypt in diesem Heft).

Drahtlose Netzverbindungen

Mobile Computer verbindet man eher über drahtlose Verbindungen (WLAN, Bluetooth, Mobilfunk) mit dem Netz als über Festverbindungen. Als Benutzer

muss man sich darauf einstellen, dass diese Verbindungen oft ohne größeren Aufwand abgehört werden können und dass dies auch geschieht. Vor der Übertragung von vertraulichen Daten (z. B. Benutzerkennzeichen, Passwörtern, Konten- oder anderen persönlichen Daten, dienstlichen Informationen) müssen Sie klären, ob die Daten vorher verschlüsselt werden müssen oder ob zumindest der gesamte(!) Übertragungsweg (SSL-)verschlüsselt und die Gegenstelle vertrauenswürdig ist (ein Server z. B., wenn er sich durch ein gültiges Zertifikat ausgewiesen hat).

Einsatz in wechselnden Netzen

Wer mit dem Notebook viel unterwegs ist und deshalb auch in fremden Netzen (z. B. in anderen Forschungseinrichtungen) eine Netzverbindung benötigt, weiß, dass es nicht überall einen unkomplizierten WLAN-Zugang gibt oder bei drahtgebundener Verbindung ein DHCP-Server automatisch eine freie IP-Adresse liefert. In manchen Netzen muss man andere VPN-Software benutzen als im HU-Netz. Für die nötigen Änderungen an der Netzwerkkonfiguration muss man Administrator (oder mindestens Mitglied der Gruppe der Netzwerkkonfigurations-Operatoren) sein. Die Nachinstallation von Netzwerk-Software gelingt ebenfalls nur als Mitglied der Administratoren-Gruppe. Um sich mit solchen Dingen nicht herumärgern zu müssen, arbeiten viele Benutzer gleich dauerhaft mit Administratorrechten und sorgen so dafür, dass Angriffe von Schadsoftware auch ganz bestimmt erfolgreich sind. Es ist also wichtig, nur in Ausnahmefällen Administratorrechte zu nutzen. Man sollte wissen, wie man Programme mit höheren Benutzerrechten starten kann (mit *„Ausführen als…“*). Einfacher ist das, wenn die Administratoren in den Instituten ihre „mobilen Benutzer“ entsprechend vorbereiten und einige Programme dafür vorkonfigurieren.

Ein weiterer Aspekt: Im HU-Netz wird ein Teil der Angriffe von außen durch eine Firewall geblockt – die Rechner in unseren lokalen Netzen sind schon dadurch in einem gewissen Maß geschützt. In anderen Netzen, vor allem an öffentlichen Orten (Bahnhöfen, Flughäfen, Restaurants), ist das nicht der Fall. Vor Angriffen (v. a. über WLAN, Bluetooth) sind Sie nur durch Vorkehrungen geschützt, die Sie selbst getroffen haben.

Erhöhte Gefahren: Verlust, Diebstahl, Beschädigung

Notebooks kann man in der Hektik auf einer Reise irgendwo liegen lassen, sie können in einem unbeobachteten Moment gestohlen werden, sie können auf den Boden fallen oder aus Versehen mit einer Flüssigkeit übergossen werden. Fast immer sind auf der Festplatte und auf mobilen Datenträgern persönliche oder dienstliche Daten gespeichert, die in der einen oder anderen Weise von Fremden missbraucht werden können. Nur selten kann man das ganz klar ausschließen. Deshalb sollten solche Daten auf mobilen Datenträgern (Notebook-Festplatten, USB-Sticks oder externen Festplatten, CDs) nur verschlüsselt gespeichert werden.

Höhere Anforderungen an die Verfügbarkeit

Ein weiterer Aspekt von Sicherheit kommt ins Spiel, wenn man an Verlust, Diebstahl oder Beschädigung denkt: Die eigene Arbeitsfähigkeit sollte auch in solchen Notfällen möglichst erhalten bleiben. Reist man zu einer Konferenz, auf der ein Vortrag zu halten ist, deponiert man wenigstens die Dateien mit dem Vortrag zusätzlich in einem anderen Gepäckstück oder an einem anderen Ort. Das Gleiche gilt für die zeitaufwendig gesammelten Daten aus einer Feldforschung. Wie man im Notfall die gesamte Installation wiederherstellen oder wenigstens die Daten retten könnte, das lesen Sie im Beitrag „Backup und Restore von PCs“.

Schlussfolgerungen

Mobile Geräte werden teilweise anders genutzt als stationäre Arbeitsplatzrechner. Deshalb sind sie unterwegs und im Netz besonderen Gefahren ausgesetzt. Das stellt sowohl an die Benutzer selbst als auch an die Administratoren der lokalen Netze höhere Anforderungen – die Mobilität hat ihren Preis:

- Für die Benutzung von Notebooks in wechselnden Netzen ist ein höheres Sicherheitsbewusstsein nötig. Über die Gefahren und die nötigen Gegenmaßnahmen sollten Sie noch besser Bescheid wissen, als es für die Arbeit an einem Rechner im HU-Netz nötig ist. Sie haben eine Verantwortung für die Daten, die Ihnen anvertraut sind. Aber nicht nur die Daten sind gefährdet, sondern auch Ihre Arbeitsfähigkeit: Infizierten Systemen wird in manchen lokalen Netzen der Zugang verwehrt (sie werden unter Quarantäne gestellt). Unter Umständen funktioniert ohnehin kein einziges Programm mehr. Ihr Rechner nützt Ihnen dann nichts mehr.
- Wer einen Computer unterwegs als zuverlässigen mobilen Begleiter braucht, muss sich schon vor der Abreise Zeit dafür nehmen, für Notfälle vorzusorgen. Dazu gehört das Anlegen von Backups, die Herstellung von Rettungsmedien, das Training von Wiederherstellungs- und Rettungsmaßnahmen, die Vorsorge gegen Diebstahl und Beschädigungen, die Verschlüsselung vertraulicher Daten, das Trainieren bestimmter Konfigurationsänderungen und das Testen aller Zugangsmöglichkeiten zum HU-Netz.
- Die Administratoren unserer lokalen Netze sollten die Notebooks der Benutzer noch „aufmerksamer“ behandeln als andere Rechner: Einerseits brauchen Benutzer mobiler Rechner mehr Unterstützung – von der Installation über besondere Konfigurationen bis zu den eben genannten „Reisevorbereitungen“. Andererseits sind mobile Rechner als besonderes Sicherheitsrisiko zu behandeln, wenn es um den Zugang zu bestimmten Diensten und Daten geht. Nicht jedes private Notebook muss unbeschränkten Zugang zum lokalen Netz bekommen und in manchen Fällen gibt es gute Gründe, mobile Rechner vom Zugang zu einem Dienst auszuschließen.